UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AIRBNB, INC., Plaintiff, v. CITY OF NEW YORK Defendant.	CIVIL ACTION NO. 18-cv-7712-PAE CIVIL ACTION NO. 18-cv-7742-PAE
HOMEAWAY.COM, INC., Plaintiff, v. CITY OF NEW YORK Defendant.	

BRIEF *AMICI CURIAE* OF LINDEN RESEARCH, INC, OFFERUP INC. AND POSTMATES INC. IN SUPPORT OF PLAINTIFFS' MOTIONS FOR PRELIMINARY INJUNCTION

BAILEY DUQUETTE P.C.
Ivo Entchev, Esq.
David I. Greenberger, Esq.
Shashi K. Dholandas, Esq.
100 Broadway, 10th Floor
New York, NY 10005
Tel: (212) 658-1946
Fax: (866) 233-5869
ivo@baileyduquette.com
david@baileyduquette.com

Attorneys for Amici Linden Research, Inc., OfferUp Inc. and Postmates Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. Civ. P. 7.1, the undersigned, counsel of record for Linden Research, Inc., OfferUp Inc. and Postmates Inc. ("*Amici*"), certifies that, as of this date:

Linden Research, Inc. has no parent corporation and no publicly held company holds more than 10% of its stock.

OfferUp Inc. has no parent corporation and no publicly held company holds more than 10% of its stock.

Postmates Inc. has no parent corporation and no publicly held company holds more than 10% of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

CONSTITUTIONAL PROVISIONS

Linden Research, Inc. ("Linden"), OfferUp Inc. ("OfferUp") and Postmates Inc. ("Postmates") by and through their counsel, Bailey Duquette P.C., respectfully submit this brief as *amici curiae* ("*Amici*") in support of Plaintiffs Airbnb, Inc.'s ("Airbnb") and HomeAway, Inc.'s ("HomeAway") motions to preliminarily enjoin the enforcement of Local Law 2018/146, New York City Admin. Code § 26-2101 *et seq.* (the "Surveillance Ordinance" or the "Ordinance").

INTEREST OF THE *AMICI*

Amici are providers of popular logistics, immersive content, communication and e-commerce platforms on the Internet, either through websites or mobile applications. Each of the *Amici* has enacted privacy policies that govern the collection and use of their respective users' data, ensuring that customers are aware of what safeguards are in place to protect sensitive information from the threat of unwanted disclosure.

Amici have a strong and direct interest in this case. Specifically, they have an interest in: (1) the continued security and privacy of their users' data, (2) fostering user confidence in such security and privacy, and (3) ensuring transparency with regard to how that data is used and protected. *Amici* also share a strong interest in ensuring that government requests for user data – both theirs and on the Internet generally – are made within the bounds of the applicable laws, including those that balance the interests of privacy, security and transparency with the interests of the government and government-directed agencies.

This action squarely implicates these concerns by presenting the question of whether a local surveillance ordinance can force an Internet platform business into an unending data sharing program with a municipal government, and arguably various governmental agencies, that undermines the fastidiously designed privacy measures that the platform has established to shield its customers' data from broad disclosures and misuse. Because *Amici* resolutely believe the

answer to that question is and must be no, they respectfully submit this brief in support of Plaintiffs' motions to preliminarily enjoin the Surveillance Ordinance.

DESCRIPTION OF THE *AMICI*

Linden develops virtual reality ("VR") platforms and immersive content catering to all demographics, allowing for millions of individuals to interact in virtual worlds and to create, share and sell their own VR experiences. Among its notable offerings are Second Life, Blocksworld and Sansar.

OfferUp is a digital marketplace where users can buy and sell goods locally. Through OfferUp's mobile application, users can post items for sale, negotiate pricing, purchase goods and make arrangements for pick-up and exchange.

Postmates is a logistics company that operates a network of couriers who deliver goods locally. Postmates' "Urban Logistics" platform connects customers with local couriers who can deliver orders from any store or restaurant.

SUMMARY OF ARGUMENT

Consumers use Internet-based applications in all aspects of their lives and share extensive information about themselves with those services in the process. Indeed, Chief Justice Roberts has observed that the proverbial Martian visitor would mistake the modern smartphone for "an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014).[1] The data stored in these applications can tell one far more about a person than any other source of information. This is an enormous convenience enabling the delivery of tailored services without precedent in human history. But it is also a grave risk and temptation to those, including the Government, who wish to exploit that information. If users lack faith that their private data will

[1] Modern smartphones store so much sensitive personal data, which implicates such broad privacy interests, that the Supreme Court has ruled that that they deserve special constitutional protections. *Riley*, 134 S. Ct. at 2494.

be responsibly handled by companies and disclosed to the Government only in exceptional circumstances – namely, pursuant to valid legal process that strikes the correct balance between user privacy and public interests in disclosure – their confidence in the online economy will be shaken and a chill will be placed on the ways in which users will associate and express themselves online.

The City of New York has enacted a surveillance ordinance that coerces online homesharing platforms into a data sharing program with the municipal government that, once in possession of that data, makes it available to an unknowable number of governmental agencies and officials. The Surveillance Ordinance obliges homesharing platforms to disclose to the municipal government, on a monthly and indefinite basis, personal and financial user data relating to customers' use of their homes for short-term rentals, together with the platforms' own confidential business records reflecting the revenues from those rentals. It does so notwithstanding – and in overt disregard of – the carefully crafted privacy measures that those platforms have established to shield their customers' data from broad disclosures and misuse.

The Ordinance constitutes Government overreach. First, it does not interpose a layer of judicial review between the Government's request and the platforms' obligation to deliver personal customer information and business records, whether in the form of an administrative subpoena or warrant; in fact, the Ordinance sets no legal standard or process whatsoever for examining the reasonableness of the Government's requests nor places any limits on government agencies' processing, dissemination and use of the obtained information. Second, the Ordinance compels homesharing platforms to obtain the "lawful consent" of their users to these continuing and unlimited disclosures in exchange for permission to use the service. N.Y.C. Admin. Code § 26-2102(b). A platform's failure to comply is punishable by severe civil penalties that can equal the

total fees collected from a non-compliant listing during the preceding year. *Id.* § 26-2104. The user's refusal to consent precludes the user's ability to use the platform, and therefore to participate in the innovative digital marketplace that platform represents.[2]

The Ordinance thus threatens to produce – even before coming into force – a ripple effect that irreparably damages essential consumer trust in privacy protection measures across the online economy. Untrammeled governmental efforts to deputize a private company to conduct vast and perpetual surveillance on the Government's behalf – including by obligating it to rewrite its privacy policies to extract user consent to such surveillance – necessarily threatens the core principles of privacy, security and transparency that lie at the heart of the digital compact between online service providers and their users.[3] In an era of rapid technological change and innovation, respect for these principles is vital to ensuring consumer trust. It is also necessary for American companies – including *Amici* – to maintain their competitive edge in the global digital economy.

Amici do not dispute that the Government may validly request information from them in pursuit of vital interests, such as the lawful investigation of crime and matters of national security. Technology companies have obligations under the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., and other laws to produce customer data to the Government with proper legal process, and *Amici* take these obligations seriously. They do and will continue to comply with reasonable, legally grounded requests for information in their possession or control pursuant to valid legal

[2] In contrast, the City of New York's long-established hotel industry is completely unaffected by this legislation.

[3] A cross-section of the technology industry filed amicus briefs echoing similar concerns in opposition to the FBI's recent attempt to use a centuries-old statute, the All Writs Act, to force Apple to build software to disable security features of the iPhone used by the perpetrators of the San Bernardino terrorist attacks. *See In the Matter of the Search of an Apple iPhone Seized During the Execution of A Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. 5:16-CM-10, 2016 WL 859874 (C.D. Cal. Mar. 4, 2016) (Dkt. No. 86) at 11. The Court is also respectfully referred to the amicus briefs filed by Google, among others, in *Patel* raising concerns about how laws such as the one at issue here adversely impact the online economy. *See* Brief for Google Inc. as Amicus Curiae Supporting Respondents (Jan. 30, 2015), *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015)

processes enacted by the legislature and consistent with federal and applicable state law.

Amici submit here, however, that the City's effort to use the Ordinance to impose on homesharing platforms the obligation to maintain a surveillance program through municipal legislation that lacks any discernible legal limits sets a dangerous and potentially far-reaching precedent that, unless enjoined, will ultimately spread to other types of online platforms. By circumventing applicable constitutional and statutory provisions that carefully balance the Government's interests in disclosure against the interests that private parties have in keeping information private and secure, the City has created a surveillance regime that is sharply out of step with (1) users' expectations of how their data will be treated under their digital compact with Internet-based service providers (this digital compact is described, *infra*) and (2) what is required under existing law.

For these reasons and those discussed below, *Amici* respectfully urge the Court to grant Plaintiffs' motions to preliminarily enjoin the enforcement of the Surveillance Ordinance.

ARGUMENT

I. THE SURVEILLANCE ORDINANCE REQUIRES ONLINE SERVICE PROVIDERS TO UNDERMINE THE BASIC PRINCIPLES GOVERNING THEIR ENGAGMENT WITH USERS

The City's efforts to force online service providers to turn over user information on a continuous and indefinite basis without any procedural protections – and without their users' true and valid consent – undermines their commitment to protect the privacy of user data, to ensure its security and to permit transparency as to its handling and use.

A. Protecting privacy, ensuring security and fostering transparency are essential principles of the digital compact between online service providers and their users

We are in the midst of a digital revolution in which a growing array of online services is empowering people to connect, create, explore and express themselves online in exciting and

unprecedented ways. *Amici* and the services they offer are participants in that revolution. Linden enables users to create, share and sell virtual reality experiences; Postmates connects customers with a network of couriers and facilitates the local delivery of goods; and OfferUp creates a digital marketplace where people can buy and sell goods locally. Other popular online services include the ability to communicate across the globe with large audiences, to publish and respond to commentary in online fora composed of particular communities and to engage in the sharing economy by deploying one's possessions, such as by renting one's home.

As more and more of these services are made available on mobile and home devices, the volume of sensitive data about consumers in the hands of online service providers has increased, as has user concern about how (and by whom) it will be used, handled and protected.

This unfolding digital revolution has meant that "privacy, which has been at the heart of our democracy from its inception," is "needed [] now more than ever." Executive Office of the President, Consumer Data Privacy in a Networked World: *A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 1 (2012)* at C3. In light of the growing risk that the privacy of personal information might be violated by a variety of state and non-state malefactors, the public has demanded ever stronger privacy and security protections. *See, e.g.*, Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission ("FTC"), *Beyond Cookies: Privacy Lessons for Online Advertising*, AdExchanger Industry Preview 2015 (Jan. 21, 2015) ("consumer awareness and demand for privacy continues to grow" and there is "even consumer reluctance to engage fully in the marketplace as a result").

In response, scores of technology companies vigorously compete on ways to make sensitive user information increasingly private and secure. The quality of the privacy and security measures that they are able to extend to their users is a core differentiator in the digital marketplace

and affects whether customers will use their services or purchase their products. *See* Scott J. Savage & Donald M. Waldman, *The Value of Online Privacy* (Univ. of Colo. At Boulder, Working Paper No. 13-02, 2013) (determining that "privacy permissions are … important characteristics a consumer considers when purchasing a smartphone app" and that consumers are willing to pay for greater privacy protections).

Ultimately, growing consumer concerns about the privacy and security of user data have given rise to a market-based digital compact between service providers and their customers that commits providers to three basic principles: to protect the privacy of their users' data, to ensure its security and to foster transparency about how that data will be handled and used. These three principles are essential to preserving consumer trust in the online economy and are incorporated as the cornerstone of the Consumer Privacy Bill of Rights. *See* Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 1* (2012) ("[c]onsumers have a right" to "[t]ransparency" about "privacy and security practices" and the "secure and responsible handling of personal data").

A serious and ever-present threat to the digital compact is unexpected government interference with privacy protections, which typically takes the form of warrantless surveillance and other overreach designed to gain access to user data for governmental ends. Government surveillance poses a unique threat to the digital compact because it is capable of producing a pronounced chill on online behavior. For example, as the warrantless surveillance by the National Security Agency of the communications of innocent Americans became public, a 2014 Harris poll showed that 47 percent of respondents "were thinking more carefully about what they do, what they say or where they go on the Internet in light of the spying revelations." Julian Hattem, "Many

Say NSA News Changed their Behavior," *The Hill*, April 2, 2014.

Amici submit that, as technological innovation continues apace, and the digital economy continues to expand, it is ever more important that there be a social commitment to maintaining and protecting – by the courts if necessary – consumer trust in this digital compact.[4]

B. *Amici* have adopted a host of protective measures in advancement of the digital compact

Amici are committed to advancing the digital compact's core principles through measures that aim to safeguard the privacy and security of their users' data. Certain federal and state agencies have guided the private sector to take these steps. The Federal Trade Commission ("FTC"), for example, has highlighted that companies that maintain user data are potential targets for malefactors and should incorporate security "into the decision making in every department of [their] business." Fed. Trade. Comm'n, Start with Security: Lessons Learned from FTC Case 2 (2015); *see also* FTC, What's the Deal? An FTC Study on Mobile Shopping Apps 6 n. 16 (2014) ("reiterat[ing] [the FTC's] call for [app] companies to practice 'Privacy by Design' and to offer consumers simplified choices over how their data is handled.") (citing FTC guidance).

Amici take care to be transparent with users in their detailed privacy policies about the data they collect and protect, to ensure that users trust that they are making informed and voluntary choices about sharing their data. *See, e.g.*, "Types of Information We Collect," Linden Privacy Policy, https://www.lindenlab.com/privacy#privacy1 ("We recognize the importance of protecting information collected from our users and have adopted this Privacy Policy to inform you about

[4] As noted by Justice Sotomayor in *United States v. Jones*, 565 U.S. 400 (2012): "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.*, 417-418 (citations omitted).

how we gather, use, process, store and disclose information, including personal information, in conjunction with you access and use of our Services."). *Amici*'s privacy policies further explain to users the uses to which user data will be put and the ways in which it will be secured. *See*, *e.g.*, "Use of Information," OfferUp Privacy Policy, https://offerup.com/privacy/).

Amici further inform their users that their personal data may be disclosed to third parties in specified circumstances, including to the Government, where the disclosure is legally required to comply with laws, regulations, legal process or a *bona fide* governmental request. *See*, *e.g.*, "How Postmates Shares Information It Collects From Users," Postmates Privacy Policy, https://postmates.com/legal/privacy ("We may share your information with third parties in the following cases: … Where disclosure is required or appropriate in order to comply with laws, regulations, legal process, or a governmental request).

The disclosures of customer-related information that the municipal government seeks in the Surveillance Ordinance, however, fail to satisfy any of *Amici*'s compulsory bases for disclosing customer-related information to the Government or to any other third party under their respective privacy policies. While *Amici* may reserve *discretion* to disclose user data upon appropriate and meritorious governmental requests, they would not voluntarily agree to the type of broad, endless and unlimited disclosures being sought in the Ordinance exactly because they are deeply damaging to the digital compact that they have with their users. Indeed, they are filing this brief to voice that precise objection.

C. The Ordinance interferes with the digital compact and creates risks related to broad access of user data by government agencies

Amici acknowledge that the importance of these three principles (protecting privacy, ensuring security and fostering transparency in connection with user data) do not – and should not – absolutely preclude the Government from seeking information about users from online service

providers in all cases. Like other technology companies, *Amici* do and will continue to comply with meritorious requests for data made in accordance with valid legal process.[5]

Indeed, *Amici* assist with investigations that are conducted pursuant to, and governed by, applicable statutory and regulatory frameworks that accord with federal and applicable state (here, New York) constitutions. This specifically includes requirements for obtaining a warrant, or issuing a subpoena, for user data in a company's possession. *See, e.g.* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 859 (2014).

In the instant case, the municipal government failed to provide such a process in the Ordinance, which it crafted to evade the Stored Communications Act ("SCA") and federal and state constitutional protections. The Ordinance is neither narrowly nor precisely tailored to minimally impair the privacy rights protected by statute and the federal and state Constitutions and does not comport with users' privacy expectations. Rather, it authorizes blanket searches without any showing of probable cause or even suspicion that a law has been violated. As explained further below, it also deputizes private homesharing platforms to help carry out the Government's surveillance program by compelling modifications of their privacy policies to extract purported waivers of basic constitutional and statutory rights from their users.

Equally damning is the purpose for which the Ordinance was passed. To *Amici*'s eyes, the Ordinance resembles an all-too-familiar protectionist reaction by an established industry – in this case, the New York hotel industry – threatened by consumers' adoption of an innovative and

[5] Companies on the scale of Amazon, Facebook and Google employ full-time teams of employees dedicated to fielding government requests for customer data. *See* Amicus Brief of Amazon et al., *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD20*, No. 5:16-CM-10, 2016 WL 859874 (C.D. Cal. Mar. 4, 2016) (Dkt. No. 86) at 11. They also publish law-enforcement guidelines that explain their products, what customer data can be requested through legal process, and how to best to serve process on the company. *Id.*

disruptive technology and seeks to erect artificial legal barriers to its success. (According to Airbnb, the user information collected under the Ordinance will be turned over to a special City of New York enforcement agency known to be working with the hotel lobby against homesharing.) *See* Airbnb Memo (Dkt. No. 14) at 1. There are no appropriate procedural safeguards in place, and it is troubling to consider what other protectionist businesses will do in the footsteps of the Ordinance to lobby for comparable legislation against companies – like *Amici* – that compete against them.

It bears emphasis that merely sharing data with the City under the Ordinance creates various security and other risks that the Government will mishandle or misuse the data. During the City's public hearings on the Ordinance, the NYCLU warned that the Ordinance "mandates the reporting of personal information … without any apparent privacy protections" and opens the door to various abuses once it is in the possession of the City. *Tr. of Minutes on Intro No. 554 and Intro No. 981 Before the Comm. On Hous. and Bldgs.* 109:14-17 (2018) (statement of B. Haroules). The NYCLU specifically highlighted the following privacy and security risks: (1) the absence of oversight and accountability for the third parties storing the data; (2) the absence of a data retention policy, which creates the likelihood of security breaches; (3) the potential for unwarranted surveillance of people whose data is turned over to the City; (4) the potential for misuse of the data by agencies applying the Government's "data crunching technologies" which are supplied by technology company Palantir, whose past clients include the CIA, ICE, DHS, the FBI and NYPD; (5) the misuse of the data for selective enforcement purposes, including immigration enforcement and targeted evictions; and (6) the absence of any anonymization of the data. *Id.* 110-113.

At a minimum, the fact that nothing expressly prevents the City from sharing the information with other agencies or third parties risks exposing it across the Government, to an

unknowable number of agencies and people, including for purposes of criminal prosecution. This alone is cause for serious concern that the data could be mishandled, misused or hacked. As the Second Circuit observed in discussing the NSA's self-imposed limits on its collection of bulk telephone metadata, the "more metadata the government collects and analyzes," the "greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals." *ACLU v. Clapper*, 785 F.3d 787, 794 (2d Cir. 2015).

This concern is particularly pressing for those *Amici* who handle significant volumes of Internet traffic and securely store personal data for a large number of people.

II. THE SURVEILLANCE ORDINANCE VIOLATES THE CONTROLLING LEGAL FRAMEWORK AND ITS DELICATE BALANCE OF POLICY CONSIDERATIONS

The Ordinance violates the public policy balance that the law strikes between the Government's interest in obtaining relevant information and the platform's and user's interests in privacy. It does so in at least two ways. First, it fails to respect the time-worn prohibition on unreasonable search and seizure as embodied in the Fourth Amendment and the New York Constitution. Second, it runs counter to, and is preempted by, the Stored Communication Act, which strikes a balance between these competing interests in the context of the digital economy.

In apparent recognition that the Ordinance would otherwise be illegal, the municipal government requires the homesharing platforms to obtain user consent to surveillance in exchange for their users' use of the platform's services. N.Y.C. Admin. Code § 26-2102(b). If the user refuses to consent, the user cannot use the platform. And if the platform fails to comply, it is subject to significant penalties. This tactic represents an insidious and dangerous attempt to invoke "user consent" to ratify the City's surveillance program. Moreover, it trivializes what should be carefully considered consent bearing on constitutional protections. Indeed, if permitted to stand,

the Ordinance effectively means that fundamental protections against Government intervention may be waived by a routine click of a button to acquire the latest app in an otherwise private transaction occurring over the Internet. As more and more businesses operate exclusively online, forfeiting such protections could become a precondition to participating in particular marketplaces, including those *Amici* engage in.

A. The Ordinance Violates the Fourth Amendment and New York Constitution

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects," and provides that "no warrant shall issue, but upon probable cause." United States Constitution, Fourth Amendment. Similarly, Article I, Section 12 of the New York Constitution protects "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." The Surveillance Ordinance's broad disclosure provisions requiring homesharing platforms to turn over customer-related business records to the City without any form of pre-compliance review violate both protections.

The Supreme Court's recent decision in *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015), directly governs the analysis here. In *Patel*, the Supreme Court invalidated on Fourth Amendment grounds a city ordinance that would have forced hotel owners to keep guest-related information and produce it on demand for inspection to law enforcement. *Id*. at 2447-48 (2015). The guest-related information involved: (1) the guest's name and address; (2) the number of people in each guest's party; (3) the guest's date and time of arrival; (4) the scheduled departure date; and (5) the rate charged. *Id*. The Court held that the Fourth Amendment protected hotels' privacy rights in this information and found that the ordinance was "facially unconstitutional because it penalize[d] [the hotel operators] for declining to turn over their records without affording them any opportunity for pre-compliance review" examining the reasonableness of the information

requests. *Id*. at 2447, 2451-54.

This logic applies with equal force here. *Patel* prohibits the City of New York from legislating a blanket request for the customer-related records at issue. And yet that is precisely what the City has done. The Ordinance requires homesharing platforms to disclose their confidential customer-related business records to the City, indefinitely and on a periodic basis, without a warrant, showing of probable cause or any opportunity for pre-compliance review. *Id*. at 2452.

Although *Patel* did not involve an online platform, its legal and policy reasoning extend to the digital arena, particularly considering the vast amounts of data collected by online services. A California district court recently applied *Patel* to a homesharing ordinance passed by the City of Santa Monica that provided for data sharing with the government. *See Homeaway.com, Inc. v. City of Santa Monica*, No. 2:16-cv-06641, 2018 WL 3013245 (C.D. Cal. Jun. 14, 2018). The ordinance there similarly required the homesharing platforms to disclose: (1) each homesharing and vacation rental in the City; (2) the names of the persons responsible for each such listing; (3) the address of each such listing; (4) the length of stay of each such listing; and (5) the price paid for each stay. Santa Monica Mun. Code ("SMMC") § 6.20.050(b).

The *Homeaway.com* court reasoned that *Patel* requires pre-compliance review to be included in the Santa Monica ordinance. *Homeaway.com*, 2018 WL 3013245 at *7-8. It then agreed with the City of Santa Monica that the ordinance imported appropriate subpoena and review provisions located elsewhere in the statute, such that there was adequate pre-compliance review. *Id*.

Here, the City of New York makes no such attempt to situate its Ordinance within a pre-compliance process provided for in the Ordinance or related municipal laws. This is because no

pre-compliance process exists. Instead, the municipal government takes the flippant position that the instant court action, which Plaintiffs brought to prevent the coming into force of an unconstitutional and unlawful surveillance regime, may once and for all satisfy the City's obligation under Supreme Court precedent to provide for any required pre-compliance review. *See* City Memo (Dkt. No. 27) at 16-17. The Ordinance of course did not contemplate this litigation as the pre-compliance review, nor did the Supreme Court intend a lawsuit to satisfy that requirement, and it cannot now be deemed the same.

Finally, the Ordinance similarly violates Article I, Section 12 of the New York Constitution, which affords even "greater protection against unreasonable searches than the U.S. Constitution." *See, e.g., 5 Borough Pawn, LLC v. City of New York*, 640 F. Supp. 2d 268, 278 (S.D.N.Y. 2009). The blanket and indefinite information requests are not "narrowly tailored" nor is the extent of their disclosure or use within the government in any way limited. *People v. Scott*, 79 N.Y.2d 474, 498-99 (1992) (holding that statutorily authorized administrative searches "must be narrowly and precisely tailored to prevent the subversion of the basic privacy values embodied in our Constitution").

B. The Ordinance Violates the Stored Communications Act

The SCA is a federal law that expressly concerns the circumstances in which Government actors should be permitted to seek and obtain electronically stored information. It extends "a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government and service providers in possession of users' private information." *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1179 (9th Cir. 2013).

The SCA provides for specific forms of process governing the disclosure to the Government of "record[s] … pertaining to a subscriber" of an Electronic Communication Service

("ECS") or Remote Computing Service ("RCS") provider, such as an online homesharing platform. 18 U.S.C. § 2703(b), (c); *see, e.g.*, *Homeaway.com, Inc. v. City of Portland*, No. 3:17-CV-00091-MO, ECF No. 36, 35:11-16 (D. Ore. Mar. 27, 2017) (Homeaway qualifies as an ECS and RCS). Whenever the Government seeks the contents of *communications*, it is obligated to do two things: first, obtain a warrant based on probable cause or provide notice to the subscriber or customer; second, either issue a subpoena authorized by a federal or state statute, or obtain a court order authorizing disclosure. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(1)(A), § 2703(b)(1)(B)(i)-(ii), (d). In the case of *any other record or information* pertaining to a subscriber or customer of a service, the government may require disclosure from an ECS or RCS provider only when the government entity obtains a court order or warrant; otherwise, the consent of the subscriber or customer to the disclosure is required. 18 U.S.C. § 2703 (c)(1)(A)-(C). In the case of more basic types of subscriber information – *i.e.*, customer name and address – the Government may proceed using a subpoena authorized by a federal or state statute. *Id*. § 2703(c)(2).

The SCA does not allow disclosure of customer records or any kind of subscriber information, no matter how basic, in the absence of a legal process. Because the Ordinance here provides for no such process, either in the form of a warrant, court order, subpoena or pre-compliance review, it conflicts with the SCA and destroys the careful public policy balance embodied therein.

Permitting the Ordinance to stand would plainly undercut the purpose of the SCA, which preempts it. *Homeaway.com*, ECF No. 36, 36:6-12 (finding likelihood of success on SCA claim because ordinance required disclosures "within the set of information that the [SCA] protects from disclosure [but without] following the procedure required by the [SCA].").

C. The City's Distorted View of Consent Would Render Fundamental Constitutional and Statutory Rights Nugatory

The Ordinance requires homesharing platforms to obtain consent from users to the governmental disclosures in exchange for use of the service. This is clearly a pretextual requirement designed to support a contention – in the face of a Fourth Amendment and SCA attack – that users have ratified the disclosures. N.Y.C. Admin Code § 26-2102(b).

Consent to the surrender of Fourth Amendment rights should be freely given, informed, and clear and unambiguous, particularly when that consent purports to be embedded in an unexpected forum, such as a private agreement expected to embody the digital compact. *See United States v. DiTomasso*, 56 F. Supp. 3d 584 (S.D.N.Y. 2014) (user maintained an expectation of privacy as against the Government despite agreeing that company's privacy policy permitted monitoring of communications); *Schnekloth v. Bustamonte*, 412 U.S. 218, 228 (1973). Requiring platforms to deliver blanket consent from their customers as a condition of using a private online service by as little as "advising or providing notice to a user of the booking service that new or continuing use of such booking service as a host constitutes consent" (N.Y.C. Admin Code § 26-2102(b)) does not meet this standard for true and genuine consent.

Indeed, the SCA establishes the appropriate and robust consent that is sufficient to authorize the disclosures contemplated by the Ordinance. It also contains a consent exception that applies only when the government entity, not the service provider, directly seeks and obtains the consent of the subscriber or customer to the particular disclosure. 18 U.S.C. § 2703(c)(1)(C); *see also Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121, 129 (D. Conn. 2004) (the SCA "clearly instructs that the burden is on the governmental entity to obtain consent."); *Corley v. Vance*, No. 15 Civ. 1800, 2015 WL 4164377 at *7, (S.D.N.Y. Jun. 22, 2015) ("[A] governmental entity seeking information from a service provider must comply with specific legal process or obtain the subscriber's consent.").

The municipal government's distorted view of valid user consent reduces the waiver of federal constitutional and statutory protections against the state to the point of dystopian fantasy, by implying that one could forfeit these rights simply by clicking a button to acquire an app. from an online vendor such as Apple or Google. Protections under the Fourth Amendment would be paltry and trivial indeed if the City could *de facto* condition a person's use of the Internet on such a casual surrender of the right to be free from unreasonable search. *See, e.g.*, *Frost v. R.R. Comm'n*, 271 U.S. 583, 593-597 (1926) (states and localities cannot condition the right of a person to do business in the state or locality on that person's waiver of federal statutory or constitutional rights); *accord Koontz v. St. Johns River Mgmt. Dist.*, 570 U.S. 595 (2013); *Sokolov v. Vill. of Freeport*, 52 N.Y.2d 341, 346 (1981) (finding it "beyond the power of the State to condition an owner's ability to engage his property in the business of residential rental upon his forced consent to forego certain rights guaranteed to him under the Constitution.").

But the City takes its dangerous view of consent even further. It argues in its submissions that that standard provisions in Airbnb's and HomeAway's privacy policies, which permit them to disclose user information pursuant to lawful requests by governmental authorities constitute the consent required for them to comply with the Ordinance. *See* City Memo (Dkt. No. 27) at 13-14. The City's argument is circular, for it contends, in sum, that a request under the Ordinance *is lawful* because users have *consented* to lawful requests for disclosure, but *consent* has only been granted under those policies on the assumption that the request is *lawful*. Neither *Amici*'s users, nor any others of which *Amici* are aware, have already consented to unlawful governmental requests for their information under a governing privacy policy.

The implications of the City's view on consent are chilling because such "consent" is capable of exposing the entirety of a person's online activities to the Government as a natural and

inevitable consequence of the user's routine use of the Internet. The Ordinance itself appears to recognize the invalidity of this form of consent – and effectively renders such consent worthless – because it separately provides that the homesharing platform's failure to obtain the valid consent of a user is not an excuse for the platform failing to turn over the requested customer record. *See* N.Y.C. Admin. Code § 26-2102(b) ("[i]t shall not be a defense to a violation of [the reporting requirement] that the booking service did not obtain consent."). Accordingly, even under the City's theory and assuming *arguendo* that the Ordinance's consent is lawful, the fact that the Ordinance still requires turnover of information in the absence of consent renders it unlawful.

Because the Ordinance fails to meet these constitutional and statutory requirements, it violates the applicable legal framework and its delicate policy balance.

III. THE SURVEILLANCE ORDINANCE DEPUTIZES PRIVATE ONLINE ACTORS TO ACT AS A FULL-TIME SURVEILLANCE ARM OF GOVERNMENT

While the Government can in some cases require private parties to support governmental information gathering techniques – for example, by requiring them to produce relevant documents or give truthful testimony through an appropriate legal process – the Government does not hold the general authority to deputize private third parties to continuously share information, or otherwise to conduct full-time surveillance or investigation of others, in the absence of legal safeguards that recognize and preserve their status as private actors. *Skinner v. Railway Labor Executives' Ass'n.*, 489 U.S. 602, 614 (1989) (a private party made to assist in a search or seizure becomes an agent of the government).

The Surveillance Ordinance blurs the line between public and private actors in several ways. *First*, it eschews the existing framework comprised of tailored and reviewable requests for private information that Congress has provided in the SCA in favor of conscripting homesharing platforms in an ongoing, full-time surveillance program devoid of the pre-compliance review that

is intended to limit governmental intrusion into private interests. As explained at length above, the SCA – preemptive federal law – was designed to balance governmental interests with user security and privacy, and withholds from the Government the very authority that the Ordinance purports to give the City of New York. In simple truth, the Ordinance ignores its obligation to treat homesharing platforms as independent, private actors with rights under the federal and state constitutions, as well as the SCA and various statutes that expressly govern how the Government, including law enforcement, may secure access to their private communications and data. *See* Wiretap Act ("Title III") (codified at 18 U.S.C. § 2510, *et seq*.); the Communications Assistance for Law Enforcement Act ("CALEA") (codified at 47 U.S.C. § 1001, *et seq*.); Foreign Intelligence Surveillance Act ("FISA") (codified at 50 U.S.C. § 1801, *et seq*.).

Second, the Surveillance Ordinance further treats homesharing platforms as instruments of the Government by requiring them to undertake affirmative acts at the behest of – and indeed in place of – the Government to aid the Government's surveillance program. The Ordinance compels otherwise unwilling private companies to rewrite the privacy policies they have carefully enacted to govern their commercial engagement with users, in order to obtain the users' consent to a potentially entirely unrelated Government data collection. This obligation goes beyond the nature and purpose of the platform's normal business activities and ignores the requirement in the SCA that "the burden is on the governmental entity to obtain consent," not the private party. *Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d at 129 . Moreover, if the platforms did not already collect this information, the implication of the Ordinance is that they would need to collect it for the City's benefit, regardless of any attendant business purposes.

Third, the Surveillance Ordinance compels these affirmative acts of assistance from unwilling private parties despite the existence of constitutional protections from such compulsion.

The Ordinance requires that homesharing platforms "advis[e] or provid[e] notice" to their users "that new or continuing use" of their platforms "constitutes consent" to the sharing of their sensitive information with the City. N.Y.C. Admin. Code § 26-2102(b). By "compelling [homesharing platforms] to speak a particular message" that they would not otherwise communicate, the Ordinance impermissibly "'alter[s] the content of [a private party's] speech'" and violates the First Amendment. *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2371 (2018) (citations and alteration omitted); *see also Evergreen Ass'n, Inc. v. City of New York*, 740 F.3d 233, 244-245 (2d Cir. 2014) ("Laws that compel speakers to utter or distribute speech bearing a particular message" are subject to "rigorous scrutiny".).

IV. IF THE SURVEILLANCE ORDER IS NOT ENJOINED, IT WILL HAVE CHILLING RAMIFICATIONS GOING FORWARD

Amici are concerned that the Surveillance Order sends a strong and dangerous message to state and local governments that they too can pass statutes or ordinances that compel digital businesses in their communities to disclose user data, notwithstanding the afforded constitutional and federal protections outlined in this brief. And, while today it is homesharing platforms being targeted, tomorrow it could be the *Amici*, or one of the countless other platforms in the expanding digital economy.

Recent events justify *Amici's* concern. As reflected in *Patel* and *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, 2016 WL 618401 (C.D. Cal Feb. 16, 2016) (No. ED 15-0451M) (Order dated Feb. 16, 2016) ("the iPhone Case"), the Surveillance Ordinance is part of a growing trend of governmental conscription of private technology companies to participate in its collection of data by forcing them to undertake the Government's surveillance or investigative tasks. In *Patel*, *supra*, the recordkeeping and warrantless inspection scheme enacted by the City

of Los Angeles required hotels to cease their practice of not retaining guest information, and disclose what they did retain to it. In the iPhone Case, the Government similarly sought to turn Apple into an investigator of the San Bernardino terrorist attacks. Purportedly relying on the All Writs Act, the Government demanded that Apple create a new product to break into its own device in violation of its promises to users, in order to obtain information contained on an iPhone belonging to one of the terrorists. *Id.* As evidenced in the large number of *amicus* briefs that poured in from across the technology sector in defense of Apple, the Government's attempt to conscript a private technology company to act as a governmental agent was seen to pose a grave threat to the independence and viability of companies in the digital economy. *In the Matter of the Search of an Apple iPhone Seized During the Execution of A Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. 5:16-CM-10, 2016 WL 859874 (C.D. Cal. Mar. 4, 2016) (Dkt. No. 60, 63, 68, 86, 94, 138, 161).

Amici further submit that it is critical that the Ordinance be preliminarily enjoined. The failure to grant a preliminary injunction could cause irreparable harm across the digital economy because the privacy and confidentiality of protected personal information might be irreversibly compromised while the availability of protections that safeguard such information is adjudicated. *See Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000) ("The harm at issue here – disclosure of confidential information – is the quintessential type of irreparable harm that cannot be compensated or undone by money damages … that is both substantial and irreversible."). As argued in I.C *supra*, once the user data is turned over to the City in the absence of appropriate restrictions on its dissemination and use, its handling within the Government will be difficult or impossible to control or to undo. In contrast, a temporary suspension in enforcement while the Court determines the legality of the Ordinance would cause no apparent harm to the City. The

Court's issuance here of an order that preliminary enjoins the Surveillance Order – which, for the reasons set forth in this brief is justifiable and appropriate – will convey a clear message to state and local governments to not pass laws that follow in the Surveillance Order's footsteps.

CONCLUSION

In sum, the erosion of consumer confidence in the manner contemplated by the Surveillance Ordinance represents a general threat to the technology industry, which has been a source of dynamic innovation and job creation in the U.S. economy. The bedrock of that confidence is the trust that consumers have placed in the digital compact regulating how their personal data will be handled by private companies and accessed by the Government. The instant motions are the latest test of whether our laws and public institutions will protect that trust.

For the foregoing reasons, *Amici* respectfully urge the Court to grant Plaintiffs' motion to preliminarily enjoin the City from enforcing the Ordinance pending this Court's determination of its constitutionality.

DATED: New York, NY
October 2, 2018

BAILEY DUQUETTE P.C.

By: /s/ Ivo Entchev

Ivo Entchev, Esq.
David I. Greenberger, Esq.
Shashi K. Dholandas, Esq.
100 Broadway, 10th Floor
New York, NY 10005
Tel: (212) 658-1946
Fax: (866) 233-5869
ivo@baileyduquette.com
david@baileyduquette.com
shashi@baileyduquette.com

Attorneys for Amici Linden Research, Inc., OfferUp Inc. and Postmates Inc.